threats or hazards that could result in substantial harm, embarrassment, inconvenience, or unfairness to any individual on whom information is maintained.

(b) *Minimum standards.* (1) Risk analysis and management planning shall be conducted for each system of records. Sensitivity and use of the records, present and projected threats and vulnerabilities, and present and projected cost-effectiveness of safeguards should be considered. The risk analysis may vary from an informal review of a small, relatively insensitive system to a formal, fully quantified risk analysis of a large, complex, and highly sensitive system.

(2) All personnel operating a system of records or using records from a system of records should be trained in proper record security procedures.

(3) Information exempt from disclosure under DCAA Freedom of Information Act Program (32 CFR part 290), shall be labeled to reflect its sensitivity, such as ''FOR OFFICIAL USE ONLY,'' ''PRIVACY ACT SENSITIVE: DISCLOSE ON A NEED-TO-KNOW BASIS ONLY,'' or some other language that alerts individuals to the sensitivity of the records.

(4) Special administrative, physical, and technical safeguards shall be employed to protect records stored or processed in an automated data processing or word processing system from threats unique to those environments.

(c) *Records disposal.* (1) Records from systems of records should be disposed of to prevent inadvertent disclosure. Disposal methods such as tearing, burning, melting, chemical decomposition, burying, pulping, pulverizing, shredding, or mutilation are considered adequate if the records are rendered unrecognizable or beyond reconstruction. Magnetic media may be cleared by degaussing, overwriting, or completely erasing.

(2) The transfer of large volumes of records (e.g., computer cards and printouts) in bulk to a disposal activity such as a Defense Reutilization and Marketing Office for authorized disposal is not a disclosure of records under this rule if volume of the records, coding of the information, or some other factor renders it impossible to recognize any personal information about a specific individual.

(3) When disposing or destroying large quantities of records from a system of records, care must be taken to ensure that the bulk of the records is maintained to prevent easy identification of specific records. If such bulk is maintained, no special procedures are required. If bulk is not maintained, or if the form of the records makes individually identifiable information easily discernible, dispose of the records in accordance with paragraph (c)(1) of this section.

Subpart C—Collecting Information About Individuals

§ 317.20 General considerations.

(a) *Collect directly from the individual.* To the greatest extent practicable, information should be collected for systems of records directly from the individual to whom the record pertains if the record may be used to make an adverse determination about the individual's rights, benefits, or privileges under Federal programs.

(b) *Soliciting the Social Security number.* (1) It is unlawful for any Federal, State, or local government agency to deny an individual a right, benefit, or privilege provided by law because the individual refuses to provide the Social Security Number (SSN). However, this prohibition does not apply if:

(i) A Federal law requires that the SSN be provided, or

(ii) The SSN is required by a law or regulation adopted before January 1, 1975, to verify the individual's identity for a system of records established and in use before that date.

(2) Before requesting an individual to provide the SSN, the individual shall be told:

(i) Whether providing the SSN is voluntary or mandatory,

(ii) By what law or other authority the SSN is solicited, and

(iii) What uses will be made of the SSN.

(3) The notice published in the FEDERAL REGISTER for each system of records containing SSNs solicited from individuals must indicate the authority for soliciting the SSNs and whether

it is mandatory for the individuals to provide their SSNs. Executive Order 9397 permits Federal agencies to solicit SSNs as numerical identifiers for individuals in Federal records systems.

(4) Upon entrance into employment with the agency, individuals must provide their SSNs; therefore, they must be given the notification. The SSN is then the individual's numerical identifier and used to establish personnel, financial, medical, and other official records. After the individual has provided the SSN to establish the records, the notification is not required when the SSN is requested only for verification or to locate the records.

(5) The Federal Personnel Manual should be consulted when soliciting SSNs for use in systems of records controlled by the Office of Personnel Management.

(c) *Collecting information about individuals from third persons.* It might not always be practical to collect all information about the individual directly from the individual, such as when:

(1) Verifying information through other sources for security or employment suitability determinations.

(2) Seeking other opinions, such as a supervisor's comments on past performance or other evaluations.

(3) Obtaining the necessary information directly from the individual will be exceptionally difficult or will result in unreasonable costs or delays; or

(4) The individual requests or consents to contacting another person to obtain the information.

(d) *Privacy Act statement.* (1) When an individual is requested to furnish information about himself or herself for a system of records, a Privacy Act statement must be provided to the individual, regardless of the method used to collect the information (forms, personal interviews, telephonic interviews, etc.). If the information requested will not be included in a system of records, a Privacy Act statement is not required.

(2) The Privacy Act statement shall include the following:

(i) The Federal law or Executive Order of the President that authorizes collecting the information.

(ii) Whether it is voluntary or mandatory for the individual to provide the requested information.

(iii) The principal purposes for which the information will be used.

(iv) The routine uses that will be made of the information (to whom and why it will be disclosed outside the Department of Defense); and

(v) The effects, if any, on the individual if all or part of the information is not provided.

(3) The Privacy Act statement must appear on the form used to collect the information or on a separate form that can be retained by the individual requesting it. If the information is collected other than by the individual completing a form, such as when the information is solicited by telephone, the Privacy Act statement should be read to the individual and a copy sent to him or her on request.

(4) It is mandatory for an individual to furnish information about himself or herself for a system of records only when a Federal law or Executive Order of the President specifically imposes a duty to furnish the information and provides a penalty, e.g., criminal sanctions, for failure to do so. If furnishing the information is only a condition for granting a benefit or privilege voluntarily sought by the individual (such as a request for annual leave), it is voluntary for the individual to give the information. However, the denial of the benefit or privilege must be listed in the Privacy Act statement as one of the effects of not providing the information, i.e., the effects on the individual if the information is not provided.

§ 317.21 Forms.

(a) *DCAA forms.* (1) DCAA Regulation 5015.3[8], ''DCAA Forms Management Program,'' provides guidance for preparing the Privacy Act statement for use with DCAA forms.

[8] Copies may be obtained, at cost, from the Defense Contract Audit Agency, ATTN: CMO, Cameron Station, Alexandria, VA 22304–6178.